



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,108	01/16/2001	Alexander Medvinsky	018926006400	8249

43471 7590 11/21/2006

GENERAL INSTRUMENT CORPORATION DBA THE CONNECTED
HOME SOLUTIONS BUSINESS OF MOTOROLA, INC.
101 TOURNAMENT DRIVE
HORSHAM, PA 19044

EXAMINER

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/765,108	MEDVINSKY, ALEXANDER	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 September 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7 and 10-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 and 10-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 9/18/06, applicant has amended claims 11, 12, 15, 16, 18, and 21-22. The following claims 1-7 and 10-23 are presented for examination.

In response to communications filed on 9/18/06, the claim objection and the 112th rejection first paragraph have been withdrawn.

Applicant's arguments, filed on 9/18/2006, with respect to the rejection of claims 1-7 and 10-23 have been fully considered but they are not persuasive. Applicant argues that Klingler's provisional does not disclose a time stamp synchronization source to synchronize cryptographic operations. As previously disclosed in the Office action, "The "timestamp" disclosed by Klingler such as encryption synch counter, and encryption switch, and additional algorithm for synchronization of cryptographic operations reads on the claimed invention." Figures 14 and 15 of Klinger illustrating the embodiments of encryption synchronization are equivalent to figure 2.3 of the provisional. Figure 14, (1402) clearly shows a "start encryption counter" that meets the recitation of a time stamp synchronization source. In addition, the diagram describes a determination is made to find out if the master encryption switch is on and the number of bytes of the message (i.e. size) to be transmitted are loaded into the counter to start the encryption synchronization process (see figure 14 and paragraphs 94-95). Figure 14, 1401 further shows the synchronization of the decrement synchronization counter with respect to the encryption synch counter: determining if the encryption synch counter is started, if the master encryption switch is on as well as information about the message and decrementing the counter by one; if the

encryption synch counter is zero, a new key is generated and the encryption is considered synch, the encryption synch counter stops (see paragraph 98 and figure 14). Therefore, as shown above, the provisional supports the citation in the reference contrarily to applicant's arguments.

With respect to Applicant's affidavit to antedate the reference, Applicant mentions that Attachment A is provided describing the invention and Attachment B is provided to show a description of the invention was provided to the law firm. None of the attachments is received by the Office with the amendment filed on 9/18/06. Applicant is also reminded that the mere submission of an affidavit is not sufficient to antedate the reference. The affidavit filed on 9/18/2006 under 37 CFR 1.131 has been considered but is ineffective to overcome the Klinger reference. The evidence submitted is insufficient to establish a conception of the invention prior to the effective date of the Klinger reference. While conception is the mental part of the inventive act, it must be capable of proof, such as by demonstrative evidence or by a complete disclosure to another. Conception is more than a vague idea of how to solve a problem. The requisite means themselves and their interaction must also be comprehended. See *Mergenthaler v. Scudder*, 1897 C.D. 724, 81 O.G. 1417 (D.C. Cir. 1897).

The affidavit or declaration and exhibits must clearly explain which facts or data applicant is relying on to show completion of his or her invention prior to the particular date. Vague and general statements in broad terms about what the exhibits describe along with a general assertion that the exhibits describe a reduction to practice "amounts essentially to mere pleading, unsupported by proof or a showing of facts" and, thus, does not satisfy the requirements of 37 CFR 1.131(b). *In re Borkowski*, 505 F.2d 713, 184 USPQ 29 (CCPA 1974). Applicant must give a clear explanation of the exhibits pointing out exactly what facts are established and relied on by applicant. 505 F.2d at 718-19, 184 USPQ at 33. See also *In re Harry*, 333 F.2d 920, 142 USPQ 164 (CCPA 1964) (Affidavit "asserts that facts exist but does not tell what they are or when they occurred.").

See MPEP § 715.07.

Therefore, conception was not established.

Where conception occurs prior to the date of the reference, but reduction to practice is afterward, it is not enough merely to allege that applicant or patent owner had been diligent. *Ex parte Hunter*, 1889 C.D. 218, 49 O.G. 733 (Comm'r Pat. 1889). Rather, applicant must show evidence of facts establishing diligence.

In determining the sufficiency of a 37 CFR 1.131 affidavit or declaration, diligence need not be considered unless conception of the invention prior to the effective date is clearly established, since diligence comes into question only after prior conception is established. *Ex parte Kantor*, 177 USPQ 455 (Bd. App. 1958).

See MPEP § 715.07(a).

Diligence need not be considered unless conception of the invention prior to the effective date is clearly established.

Applicant has not overcome the rejection as shown above in view of the prior art and it remains the Examiner's position that claims 1-7 and 10-23 remain rejected.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 6-7, 10-16, and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2003/0003896 to **Klingler et al** in view of US Patent 5,081,679 to **Dent**.

As per claims 1 and 19, **Klingler et al.** discloses a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network; the system comprising: Klinger discloses in one embodiment a system comprising remote units and base stations for sending/receiving messages, messages include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026; and fig. 14-15) that meets the recitation of a local multimedia terminal adapter receiving the voice packets having a timestamp as a synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter, the local multimedia terminal adapter comprising, a local key stream generator for generating a first key stream, for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets, forwarding the encrypted voice packets from the local location to the remote location for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-

0094); the remote multimedia terminal adapter receiving the encrypted voice packets, the remote multimedia terminal adapters further comprising, a remote key stream generator for generating the first key stream in order to decrypt the encrypted voice packets, for example (see page 3, paragraphs 0039-0041; page 2, paragraphs 0027, 0032, 0033); and a packet decryptor decrypting the encrypted voice packets using the first key stream, for example (see page 3, paragraphs 0039-0041; page 2, paragraphs 0027, 0032, 0033), wherein both key stream generators are capable of generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session and the packet encryptor and packet decryptor use the second key stream, for example (see page 8, paragraph 0101). The “timestamp” disclosed by **Klingler** such as encryption synch counter, and encryption switch, and additional algorithm for synchronization of cryptographic operations reads on the claimed invention. To provide further support of some of well known features, **Dent** in an analogous art teaches a encryption/decryption system for bit synchronization using a timeout parameter and counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). **Dent** also discloses using real-time clock and counters because it is important for the receiver to be operated in synchronism with the transmitter key stream generator for the message to be properly decoded (column 12, lines 23-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide timestamp synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter as taught by **Dent**. This modification would have been obvious because one skilled in the art would have

been motivated by the suggestions provided by **Dent** so as to enable the receiver to be operated in synchronism with the transmitter key stream generator for the message to be properly decoded (column 12, lines 23-51).

As per claims 2 and 20, Klingler et al. discloses the limitation of wherein the second key stream is generated when the system switches from a first to a second coder/decoder for compression/decompression of the voice packets, for example (see page 8, paragraphs 0100-0101 and page 10, claims 18-21).

As per claim 3, Klingler et al. discloses the limitation of wherein the second key stream is generated when a Message Authentication Code algorithm change occurs, for example (see page 6, paragraphs 0086-0089; pages 1-2, paragraph 0026 and page 10, claims 18-21).

As per claim 6, Klingler et al. discloses a system for communicating Real Time Protocol voice packets between a local and a remote location over an Internet protocol network, the system comprising: a stream cipher module for encrypting the voice packets, for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); and a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system switches from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the

synchronization of the key stream, for example (see pages 6-7, paragraphs 0086-0090; page 8, paragraphs 0101-0103 and page 10, claims 18-21, 33 and abstract). Klingler discloses voice messages that include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026) that meets the recitation of wherein the voice packets having a timestamp as a synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter. The "timestamp" disclosed by Klingler such as encryption synchronizer, and encryption switch, and additional algorithm for synchronization of cryptographic operations reads on the claimed invention. To provide further support of some of well known features, **Dent** in an analogous art teaches an encryption/decryption system for bit synchronization using timeout parameter and counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). **Dent** also discloses using real-time clock and counters because it is important for the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide timestamp synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter as taught by **Dent**. This modification would have been obvious because one skilled in

the art would have been motivated by the suggestions provided by **Dent** so as to enable the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51).

As per claim 7, Klingler et al. discloses the limitation of wherein the first communication parameter is a first coder/decoder that compresses/decompresses the voice packets, and the second communication parameter is a second coder/decoder that compresses/decompresses the voice packets, for example (see page 2, paragraph 0032).

As per claim 10, Klingler et al. discloses the limitation of further comprising a new time stamp sequence generated when the second Real Time Protocol key stream is generated, for example (see page 7, paragraphs 0093-0094).

As per claim 23, Klingler et al. discloses the limitation of further comprising a synchronization source for synchronizing and enabling decryption of the voice packets at the remote location, for example (see pages 1-2, paragraph 0026).

As per claim 13, Klingler et al. discloses a method for securely transmitting Real Time Protocol voice packets from a local to a remote location via a communication network, the method comprising: generating a first Real Time Protocol key stream for encrypting the voice packets; forwarding encrypted voice packets to the remote location, for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); generating a second Real Time

Protocol key stream for encrypting the voice packets in response to a request to change communication parameters for the same media stream, for example (see pages 6-7, paragraphs 0086-0094; page 8, paragraphs 0101-0103 and page 10, claims 18-21, 33 and abstract); and forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location, for example (see page 8, paragraphs 0101-0103). Klinger discloses voice messages that include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026) that meets the recitation of wherein the voice packets having a timestamp as a synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter. **Dent** in an analogous art teaches a system for bit synchronization using a timeout parameter a handoff counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). **Dent** also discloses using real-time and counters because it is important for the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klinger et al** to provide timestamp synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter as taught by **Dent**. This modification would have been obvious because one skilled in the art would

have been motivated by the suggestions provided by **Dent** so as to enable the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51).

As per claim 14, Klingler et al. discloses the limitation of further comprising reinitializing a time stamp for synchronizing decryption of the voice packets, for example (see pages 1-2, paragraph 0026).

As per claims 11, 15, and 21, Klingler et al. discloses the limitation of providing key derivation or a pseudorandom function based on a counter, and shared secret key, for example (see page 7, paragraph 0089, 0094; page 8, paragraphs 0101-0105) that meets the recitation of wherein the second key stream is generated by re-executing the following key derivation function: $F(S, \text{"End-End RTP Key Change } \langle N \rangle")$ where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session; $F()$ is a one-way pseudo-random function used for the purpose of key derivation; S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints or a trusted server, and "End-End RTP Key Change $\langle N \rangle$ " is a label that is used as a parameter to the key derivation function $F()$, $\langle N \rangle$ stands for an ASCII representation of a decimal number, representing a counter. **Klingler et al.** discloses the same result and also discloses algorithm for key generation in pages 4-5. Similar algorithm in the claimed invention of f as a function of a secret key and a parameter can be found in cryptography textbook known in the art, which does not depart from the spirit and scope of the invention disclosed by **Klingler et al. Dent** in an

analogous art teaches a system for bit synchronization using a timeout parameter a handoff counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide a key generation as a function of a secret key and a counter as taught by **Dent**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Dent** so as to selectively change the parameter to fit individual circumstances.

Claims 12, 16, and 22 are similar to the rejected **claims 11, 15, and 21** except for adding a source identifier, which is known in the art as found in US patents 6,2754,71 and 6,122,665. **Klingler et al.** also uses an identifier to identify the source of the message, for example (see page 2, paragraph 0032). Therefore, **claims 12, 16, and 22** are rejected on the same rationale as the rejection as the rejection of **claims 11, 15, and 21**.

3. **Claims 4 and 5** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2003/0003896 to **Klingler et al** in view of US Patent 5,081,679 to **Dent** as applied to claim 1 above and further in view of US Patent Publication US 2002/0031126 to **Crichton et al.**

As per **claims 4 and 5**, **Klingler et al.** substantially teaches forwarding/receiving encrypted packets from a local to a remote end, for example (see page 10, claims 18-21).

Klingler et al. does not explicitly teach using a gateway controller, which is well known in the art of Internet Protocol network for connecting different protocol networks. However, **Crichton et al.** in an analogous art teaches a system for bit synchronous network communications over packet networks including Internet protocol network using gateways in an end-to-end communication path to perform analog to digital conversion and to communicate with packet network in a manner known in the art, for example (see page 5, paragraphs 0042 and 0047; see also background). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a gateway controller as taught by **Crichton et al.** for forwarding and receiving encrypted packets through an Internet protocol to perform analog to digital conversion and to communicate with packet network in a manner known in the art. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Crichton et al.** so as to perform analog to digital conversion and to communicate with packet network in a manner known in the art.

4. **Claims 17 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2003/0003896 to **Klingler et al.** in view of US Patent Publication US 2002/0031126 to **Crichton et al.** and in view of US Patent 5,081,679 to **Dent**.

Claim 17 contains some of the limitations of claims 6 and 13 except for sending encrypted data to a gateway, which was discussed in claims 4 and 5 above. Claim 17 also adds generating a second Real Time Protocol key stream for encrypting the voice packets in response

to a collision detection wherein the multimedia terminal adapters have the same source identifier.

Klingler et al discloses using exiting command and control messages in a data stream for automatic synchronization if the data path has been compromised and a new connection established, and new key needs to be generated upon resynchronization. Although **Klingler et al** does not specify collision as an example for resynchronization, it does not depart from the spirit and scope of the invention disclosed by Klingler; it is obvious to one of ordinary skill in the art that collision is one of the reasons of starting new session that requires resynchronization, this is a well known feature as explained, for instance in RFC 1189. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Klingler et al to regenerate new key upon restarting a new session including in response to collision because if a new key is not generated upon resynchronization the system would be compromised for attack as suggested by Klingler et al (page 8, paragraph 101). Klingler also quotes, “the process of synchronization must give an attacker no specific knowledge of the key at any time” (provisional application). **Dent** discloses the generation of new key when there is no synchronization, as discussed in claims 11, 15, and 21. Therefore claim 17 is rejected on the same rationale as the rejection of claims 4-6 and rejection of claims 11, 15, and 21.

Claim 18 is similar to the rejected **claims 12, 16, and 22**. Therefore, **claim 18** is rejected on the same rationale as the rejection of **claims 12, 16, and 22**.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

Art Unit: 2136

system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
November 17, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11/17/06